Amendments to the Claims:

This listing of claims will replace all prior versions and listing of claims in the application:

Listing of Claims:

Claim 1 (Currently Amended): In quantum cipher communication using a light signal, a quantum cipher communication system characterized ~~by the step of~~ in that:

it uses a phase difference between a signal light and a reference light which have orthogonal polarizations for a signal of privacy key, wherein said phase difference is produced by a sender and a recipient adding a phase on the signal light or the reference light;

it has an optical balanced homodyne detector which detects said phase difference as a difference signal of the detector, wherein the phase difference is determined by comparing said difference signal with a threshold value; and

wherein ~~detecting~~ an eavesdropping ~~based on~~ is detected by the recipient measuring a change in a quantum-mechanical probability distributions of ~~two amplitude components which are 90degrees phase apart from each other by a recipient using a difference signal derived from a signal light which change is produced~~ said difference signal, which is produced by the eavesdropping operation.

Claim 2 (Original): A quantum cipher communication system as set forth claim 1, in said quantum cipher communication, characterized by the steps of:

splitting a light signal from a transmission source side into an intense reference signal and a weak transmission signal which is so weak that a change in its quantum mechanical state is detectable;

imparting a phase difference between said reference signal and said transmission signal while they are in a process of transmission;

superimposing in a transmission receiving side said reference signal and said transmission signal to form two output lights which are opposite in phase and producing a difference signal which is represented by a difference between said two output lights;

deriving a frequency distribution of said difference signal as a function of a fluctuation of the quantum state of said transmission signal;

based upon or in accordance with the frequency distribution of said difference signal, making privacy (secret) keys respectively at said transmission source and receiving sides for holding in common thereby; and

directly observing the fluctuation of the quantum state of said transmission signal.

Claim 3 (Previously Presented): A quantum cipher communication system including:

a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal;

a phase modulating means for imparting a phase modulation to said transmission signal;

a light attenuator for converting only said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable; and

a phase modulating means for imparting a phase modulation to said reference signal, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals:

a second beam splitter for superimposing said phase-modulated weak transmission signal and said phase modulated intense reference signal to form two output lights;

a first and a second photoelectric conversion elements for converting said two output lights from said second beam splitter into two corresponding electric signals which are opposite in phase; and

an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage.

Claim 4 (Original): A quantum cipher communication system as set forth in claim 3, characterized in that said phase modulating means includes a mirror movable by a distance as small as the wave length of an incident light.

Claim 5 (Original): A quantum cipher communication system as set forth in any one of claims 1 to 4, characterized in that said reference signal and said transmission signal are split both in time and as polarized and then transmitted to travel along a common path.

Claim 6 (Previously Presented): A quantum cipher communication system including:

a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal;

a first light polarizer for polarizing said transmission signal through longer one of two distance paths;

a light attenuator for converting only said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable;

a first phase modulating means for imparting a predetermined phase modulation to said transmission signal; and

a first polarized beam splitter for receiving said intense reference signal having passed through shorter one of two distance paths and said transmission signal and returning the received signal to travel along a common optical path, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals and included in a transmission receiving side:

a second polarized beam splitter for isolating from each other said transmission and reference signals transmitted through a single optical fiber;

a second phase modulating means for imparting a phase modulation to said isolated transmission signal through shorter one of two distance paths; and

a second light polarizer for polarizing said isolated reference signal through longer one of two distance paths, said system further including:

a second beam splitter for superimposing said transmission and reference signals which are coincident with each other in time and polarization to produce two output lights;

a first and a second photoelectric conversion elements for converting said two output lights into corresponding electric signals which are opposite in phase; and

an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage.

Claim 7 (Original): A quantum cipher communication system as set forth in claim 6, characterized in that a third light polarizer is provided in an output side of said optical fiber for making a correction for a disturbance of polarization of said reference signal.

Claim 8 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that threshold values are established, respectively, for positive and negative values of said difference signal, and that the state of said transmission signal is discriminated on the basis of said threshold values.

Claim 9 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as described and having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference signal and said transmission signal which develops by reason of an external cause.

Claim 10 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that such phase modulations are so imparted as described and including those for transmitting privacy keys and those with values later determined are randomly repeated.

Claim 11 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal.

Claim 12 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal.

Claim 13 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that said two output lights are converted into corresponding electric signals through photoconductor diodes.

Claim 14 (Previously presented): A quantum cipher communication system as set forth in claims 1-4, 6 or 7, characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm.

Claim 15 (New): In quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus, characterized in that

the sender's apparatus comprises of:

a light source for a laser beam;

a beam splitting means for splitting said laser beam into a signal light and a reference light;

a phase modulation means making a phase change for every light which is either of said signal light or said reference light; and

a light attenuation means for attenuating said signal light intensity,

the recipient's apparatus comprises of:

a phase modulation means making a phase change for every light which is either of said signal light or said reference light transmitted from the sender's apparatus through the transmission path;

a superimposing means for superimposing said signal light and said reference light, either of which is phase changed by said modulation means of the recipient's apparatus;

a pair of photo-detector for converting two output lights from said superimposing means into respective electric signals; and

an amplifying means for amplifying a difference signal between said electric signals,

wherein the sender, by using said phase modulation means of sender's apparatus, imparts for every light a phase change randomly selected from a set of phase changes predetermined by the sender and the recipient, and the recipient, by using said phase modulation means of recipient's apparatus, imparts for every light a phase change randomly selected from said set of phase changes, as well as measures for every light said difference signal between the electric signals amplified by the amplifying means;

then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient for every light;

the sender calculates the total phase difference between the signal light and the reference light by adding the phase change notified by the recipient and the phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference satisfy a condition predetermined by the sender and the recipient, as a raw key for candidate being adopted as a privacy key;

then the recipient, for said every light notified as a raw key for candidate, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less than the predetermined threshold value - X, whereby the recipient gets a privacy key;

the sender, for said every light making notified as a raw key for candidate, assigns bit 1 or 0 according to a condition regarding the total phase difference, which is predetermined by the sender and the recipient, whereby the sender gets a privacy key; and

wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and -X.

Claim 16 (New): In quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus, characterized in that

the sender's apparatus comprises of:

a light source for a laser beam;

a beam splitter for splitting said laser beam into a signal light and a reference light;

a movable mirror making a phase change for every said signal light ; and

a light attenuator for attenuating said signal light intensity,

the transmission path comprises a pair of paths for transmitting said signal light and said reference light respectively,

the recipient's apparatus comprises of:

a movable mirror making a phase change for every said reference light transmitted from the sender's apparatus through one of the path of transmission;

a beam splitter for superimposing said signal light transmitted from the sender's apparatus through the other path of transmission and said reference light phase changed by said movable mirror of the recipient's apparatus;

a pair of photoconductive diodes for converting two output lights from said beam splitter into respective electric signals; and

a charge sensitive amplifier for amplifying a difference signal between said electric signals, and

wherein the sender, by using said movable mirror of sender's apparatus, randomly imparts phase changes 0,90,180,or 270 degrees for said every signal light, and the recipient, by using said movable mirror of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for said every reference light, as well as measures said difference signal between the electric signals amplified by the charge sensitive amplifier;

then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light;

the sender calculates the total phase difference between the signal light and the reference light by adding said phase change notified by the recipient and said phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate being adopted as a privacy key;

then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference signal measured is equal or less than the predetermined threshold value - X, whereby the recipient gets a privacy key;

the sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key; and

wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and -X.

Claim 17 (New): In quantum cipher communication using a light signal, a quantum cipher communication system having a sender's apparatus, a recipient's apparatus and a transmission path connecting between the sender's apparatus and the recipient's apparatus, characterized in that

the sender's apparatus comprises of:

a light source for a linearly polarized pulsed light;

a beam splitter for splitting said linearly polarized pulsed light into a signal light and a reference light;

a long optical path comprising a half wave plate for rotating the polarization of said signal light by 90 degrees, a light attenuator for attenuating said signal light intensity, a phase modulator for changing the phase of said signal light and mirrors; and

a first polarized beam splitter for returning said signal light transmitted through said long optical path and said reference light onto a common optical axis, wherein said signal light and said reference light returned to the common optical axis have a mutual time delay based on the optical path length difference between said long optical path for the signal light and a short optical path where said reference signal reaches to the first polarized beam splitter from the beam splitter, and have mutually orthogonal polarizations,

the optical fiber comprises a single mode optical fiber connected to said first polarized beam splitter, wherein said signal light and said reference light are transmitted through said single mode optical fiber keeping said time delay and said polarizations,

the recipient's apparatus comprises of:

a second polarized beam splitter for splitting said signal light and said reference light transmitted through the single mode optical fiber;

a long optical path comprising a half wave plate for rotating the polarization of said reference light and mirrors, and a short optical path comprising a phase modulator for making a phase change for every signal light transmitted through the single mode fiber, wherein the time delay based on the optical path length difference between

said short optical path and said long optical path of the recipient's apparatus has the same absolute value and opposite sign to said time delay in the sender's apparatus;

a third polarized beam splitter for superimposing said signal light transmitted through the short optical path and said reference light transmitted through the long optical path;

a pair of photoconductive diodes for converting two output lights from said third polarized beam splitter into respective electric signals; and

an amplifier for amplifying a difference signal between said electric signals, and

wherein the sender, by using said phase modulation means of sender's apparatus, randomly imparts phase changes 0,90,180,or 270 degrees for every signal light, and the recipient, by using said phase modulation means of recipient's apparatus, randomly imparts phase change 0 or 90 degrees for every reference light, as well as measures said difference signal between the electric signals amplified by the amplifying means;

then, by using a public communication line, the recipient notifies to the sender said phase changes imparted by the recipient whether it is 0 or 90 degrees for every reference light;

the sender calculates the total phase difference between the signal light and the reference light by adding said phase change notified by the recipient and said phase change imparted by the sender for every light, and notifies to the recipient the lights whose total phase difference is either 0 or 180 degrees, as a raw key for candidate being adopted as a privacy key;

then the recipient, for every light notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when said difference signal measured is equal or greater than a predetermined threshold value +X, and assigns bit 0 when said difference measured is equal or less than the predetermined threshold value - X, whereby the recipient gets a privacy key;

the sender, for every light making notified as a raw key for candidate being adopted as a privacy key, assigns bit 1 when the phase imparted by the sender is 0 or 90 degrees, and assigns bit 0 when the phase imparted by the sender is 180 or 270 degrees, whereby the sender gets the privacy key, and

wherein the sender and the recipient can get the privacy key in common with suitable effective detection efficiency and suitable error rate by selecting said threshold value +X and -X.

Claim 18 (New): A quantum cipher communication system as set forth in claim 17, characterized in that a third light polarizer is provided in an output side of said single mode optical fiber for making a correction for a disturbance of polarization of said reference signal.

Claim 19 (New): A quantum cipher communication system as set forth in any one of claims 15 to 17, characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference signal and said transmission signal which develops by reason of an external cause.

Claim 20 (New): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that such phase modulations are so imparted as including those for transmitting privacy keys and those with values later determined are randomly repeated.

Claim 21 (New): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal.

Claim 22 (New): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal.

Claim 23 (New): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm.

Claim 24. (New): A quantum cipher communication system as set forth in any one of claims 15 to17, characterized in that the said signal light has a typical intensity corresponding to a single photon or so, and said reference light has a typical intensity corresponding to photons as large as 10 millions in number.